3 システムのセットアップ

本体を設置し、ケーブルを接続したあと、システムのセットアップをします。システムのセットアップは購入後、初めてセットアップする場合と再セットアップする場合に分けて説明しています。

初めてのセットアップ

購入後、初めてシステムをセットアップする時の手順について順を追って説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」は装置を導入するために最低限必要となる設定情報が保存されたセットアップ用のフロッピーディスクです。

「初期導入設定用ディスク」は、添付の初期導入設定用ディスクにある「初期導入設定ツール」を使って作成します。初期導入設定ツールは、Windows 2000、Windows NT、またはWindows Me/98/95で動作するコンピュータで動作します。

初期導入設定プログラムの実行と操作の流れ

Windowsマシンを起動して、次の手順に従って初期導入設定用ディスクを作成します。

1. Windowsマシンのフロッピーディスクドライブに添付の初期導入設定用ディスクをセットする。
2. フロッピーディスクドライブ内の「初期導入設定ツール(startupConf.exe)」をエクスプローラなどから実行する。

   [Linuxビルドアップサーバ初期導入設定ツール]が起動します。プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。

   必須情報が入力されていない場合や入力情報に誤りがある場合は、次へ進むときに警告メッセージが表示されます。項目を正しく入力し直してください。入力事項については、この後の説明を参照してください。

   すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。
3. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「システムのセットアップ」に進む。

   初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。

各入力項目の設定

[Linuxビルドアップサーバ初期導入設定ツール]で入力する項目について説明します。

パスワード設定

システムのセットアップ完了後、管理PCからWebブラウザを介して、システムにログインする際のパスワードを設定します。
この画面にある項目はすべて入力する必要があります。
パスワードは推測されにくく覚えやすいものを用意してください。

パスワードは画面に表示されません。タイプミスをしないよう注意してください。

設定済みパスワード

初めて設定する場合は、同梱の別紙「rootパスワード」に記載されたパスワードを入力してください。以前に設定を行っている場合は、設定されているパスワードを入力してください。

パスワード

設定するパスワードを入力してください。ここで入力したパスワードは、管理者(admin)でログインする場合に必要となります。パスワードを忘れたり、不正に利用されたりしないように、パスワードの管理は厳重に行ってください。

なお、パスワードを変更したくない場合は、既存パスワードと同一のパスワードを新パスワードとして設定してください。

パスワード再入力

パスワードの確認用です。パスワードと同一のものを入力してください。

ネットワーク設定　～LANポート1(標準LAN)用～

LANポート1(標準LAN)のネットワーク設定をします。[セカンダリネームサーバ]以外は必ず入力してください。

ホスト名(FQDN)

ホスト名を入力してください。入力の際には、FQDNの形式（マシン名.ドメイン名)の形式で入力してください。また、英字はすべて小文字で指定してください。大文字は使用できません。

IPアドレス

1枚目のNIC(LANポート1(標準LAN))に割り振るIPアドレスを指定してください。

サブネットマスク

1枚目のNIC(LANポート1(標準LAN))に割り振るサブネットマスクを指定します。

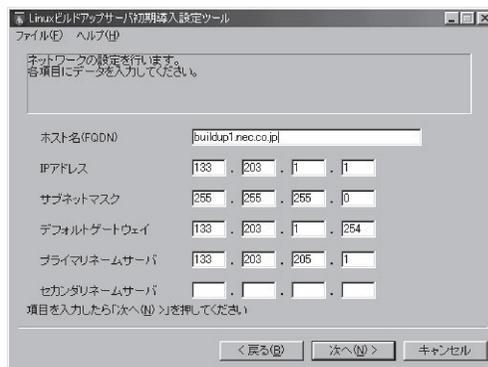
ディフォルトゲートウェイ

ディフォルトゲートウェイのIPアドレスを指定します。

プライマリネームサーバ

プライマリネームサーバのIPアドレスを指定します。

セカンダリネームサーバ

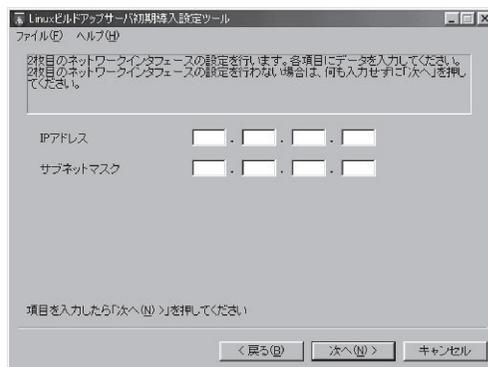
セカンダリネームサーバが存在する場合は、そのIPアドレスを指定します。

ネットワーク設定　～LANポート2(拡張LAN)用～

LANポート2(拡張LAN)のネットワーク設定をします。使用しない場合は、設定する必要はありません。

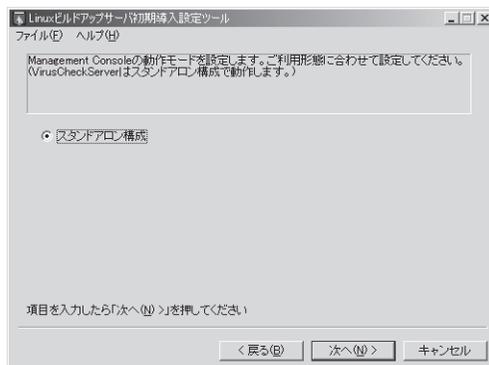
IPアドレス

2枚目のNIC(LANポート2(拡張LAN))に割り振るIPアドレスを指定してください。

サブネットマスク

2枚目のNIC(LANポート2(拡張LAN))に割り振るサブネットマスクを指定します。

初期導入設定プログラムでは増設ボードにより拡張したLANの設定を行うことはできません。Management Consoleのネットワーク設定にあるインタフェースで設定を行ってください。

システム構成条件の設定

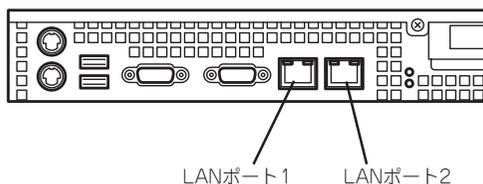
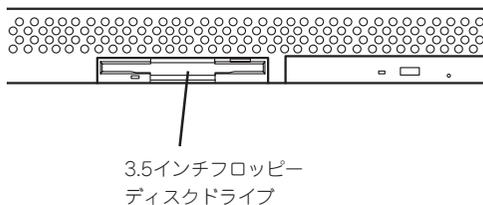
Management Consoleの動作モードを設定します。
VirusCheckServerは[スタンドアロン構成]で動作します。

システムのセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用して、短時間でセットアップできます。

セットアップの手順

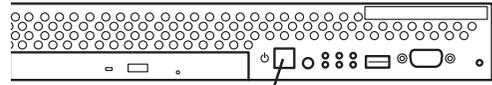
以下手順でセットアップをします。

正しくセットアップできないときは、次ページ、および137ページを参照してください。

1. 本体背面のLANポート1とLANポート2(使用する場合)にネットワークケーブルが接続されていることを確認する。

2. 前述の「初期導入設定用ディスクの作成」で作成した初期導入設定用ディスクを3.5インチフロッピーディスクドライブにセットする。

3. POWERスイッチを押す。

POWERランプが点灯します。

しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2〜3分ほどでセットアップが完了します。

次項および4章を参照してシステムの状態確認や設定変更を行ってください。

重要

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に再利用することができます。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、ビープ音を鳴らすことでユーザーに異常を知らせます(自動的に電源がOFF(POWERランプ消灯)になります)。正常にセットアップが完了しなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容をコンピュータの「メモ帳」などのツールを使って確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成し直してください。

<主なログの出力例>

■ 「Info: completed.」

→ 正常にセットアップが完了した場合に表示されます。

■ 「Info: quitting with no change.」

→ 初期導入設定ツールを使って再度作成せずに、一度セットアップに使用した初期導入設定用ディスクを再使用した場合に表示されます(設定は反映されません)。

■ 「Cannot get authentication: root」

→ 初期導入設定用ディスク中のパスワードの指定に誤りがある場合に表示されます。

■ 「Error: invalid file: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

■ 「Error: cannot open: /mnt/floppy/linux.aut」

→ 初期導入設定用ディスク中のパスワード情報を格納したファイル(linux.aut)が正しく作成されなかった場合に表示されます。

セットアップや運用時のトラブルについての対処を137ページで詳しく説明しています。

セットアップの確認

インストールされているInterScan VirusWallは初期設定値に従って動作するように設定されていますが、パターンの配信サーバへの登録など少なくとも1回はInterScanコンソールを開き、設定内容を確認するようにしてください。

重要 **InterScan VirusWallの詳細な設定は基本ライセンスに添付の「InterScan VirusWall管理者ガイド」を参照してください。**

1. InterScanコンソールを開く。

   InterScanコンソールを開くには次の2つの方法があります。

   - Management Consoleからサービスのアイコンを選択し、[ウイルスチェック]をクリックする。
   - Webブラウザを起動し、ポート番号(:1812)を付けたInterScanのURLを入力する。

     IPアドレスの部分は、 InterScanマシンのドメイン名、 IPアドレスのいずれでもかまいません。次に例を示します。

     http://ドメイン名:ポート/interscan
http://isvw.widget.com:1812/interscan
http://123.12.123.123:1812/interscan

2. InterScanコンソールにログインするためのユーザ名とパスワードを入力する。

   InterScanコンソールにはパスワードが設定されています。初期設定では、ユーザ名、パスワードともに adminが設定されています。

   重要

   以降の各設定ページで項目を変更した際には、[Apply]をクリックして、設定を保存してください。

   [Apply]をクリックせずにブラウザを終了したり、他のページを表示すると、変更が取り消されます。[Cancel]をクリックすると、各項目は設定変更前の値に戻ります。

ウイルスパターンファイル

ウイルスを検出するために、InterScan VirusWallでは、一般にウイルスパターンファイルと呼ばれる、ウイルスシグネチャの大規模なデータベースを利用しています。新しいウイルスが作成され、世間に送り出され、検出されると、トレンドマイクロ社ではそのシグネチャを収集して、ウイルスパターンファイルに情報を追加します。ウイルスパターンファイルの命名規則は次のとおりです。

lpt$vpn.###

###は、バージョン番号(たとえば505)を表します。同じディレクトリに複数のファイルが存在する場合、最も大きな番号のファイルのみが使用されます。
トレンドマイクロ社では、ほぼ毎週新しいウイルスパターンファイルを提供していますので、少なくとも数週間ごとにパターンファイルをアップデートするようにしてください。登録ユーザは、無料でアップデートファイルを入手できます。アップデートファイルは、インターネット経由で自動的にダウンロードすることができます。

古いパターンファイルを削除する必要はなく、また新しいファイルを使用するために、特別なインストール手順を実行する必要はありません。後述の[Update Virus Pattern Now]をクリックするだけで、システムが自動的に新しいパターンファイルを設定します。

ウイルスパターンファイルを手動でアップデートする

ウイルスパターンファイルを手動でアップデートするには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。

   画面には現在のパターンファイルのバージョンと、前回のアップデート日時が表示されています。

   重要

   ウイルスパターンアップデートのためのユーザ登録を実行していない場合には、ウイルスパターンファイルをアップデートする前に、[Register for Virus Pattern Updates]画面からユーザ登録を実行してください。

2. [Update Virus Pattern Now]をクリックする。

   トレンドマイクロ社の提供するパターンファイルがInterScanサーバ上のファイルよりも新しい場合にのみ、アップデートが実行されます。

ウイルスパターンファイルの自動アップデートを設定する

自動アップデートを設定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。

2. [Set Automatic Update Time]をクリックする。

   自動アップデートのためのオプションを設定する[Set Automatic Update Time]画面が表示されます。

3. **<ウイルスパターンファイルの自動アップデートを無効にする場合>**

   [No automatic update]を選択する。

   <ウイルスパターンファイルの自動アップデートを実行する場合>

   必要に応じて周期オプションを選択する。
   また、必要に応じて、[Start time]でアップデートを実行する時刻を選択してください。

HTTPプロキシサーバの使用

InterScanでは、インターネット上のトレンドマイクロ社のサイトから、新しいウイルスパターンファイルを取得します。InterScanとインターネットの間に HTTPプロキシサーバが設定されている環境で、このサイトにアクセスする場合には、HTTPプロキシサーバを指定して、プロキシサーバにログオンするための情報を指定する必要があります。

Trend Virus Control System(以降、「Trend VCS」と省略します)エージェントはTrend VCS サーバにアクセスする際に、同じプロキシサーバ情報を使用します。

プロキシサーバを指定するには、次の手順に従ってください。

1. InterScanコンソールを開き、[Pattern Update]をクリックする。

2. [Set Proxy Server]をクリックする。

   [Set Proxy for Update Virus Pattern From Internet]画面が表示されます。

3. InterScanとインターネットの間にプロキシサーバが存在する場合は、[Use proxy server for pattern download]を選択する。

   プロキシサーバが存在しない場合は、初期設定のまま[Do not use proxy server for pattern download]をチェックしておく。

   a. [proxy]に、プロキシサーバのドメイン名(またはIPアドレス)を入力します(例: proxy.company.com)。

   b. [port]にプロキシサーバが使用するポート番号を入力します(例: 80または8080)。

4. プロキシサーバにログインする際に InterScanが使用するユーザIDとパスワードを、それぞれ[User ID]、[Password]に入力する。

検索エンジンのアップデート

トレンドマイクロ社では継続的にInterScanの検索エンジンを見直し、新しい機能や機能改善を追加しています。更新された検索エンジンは、トレンドマイクロ社のダウンロードサイトに登録されます。検索エンジンを自動的にアップデートすることはできません。検索エンジンをアップデートする場合は、以下のURLから検索エンジンをダウンロードし、/etc/iscanディレクトリにコピーしてください。

http://www.trendmicro.co.jp

検索エンジンのアップデート手順

1. トレンドマイクロ社のWebサイトから InterScan VirusWall for UNIX(Linux版)の検索エンジンをダウンロードしてフロッピーディスクに保存する。

2. VC300aのFDDをマウントする。

   ① VC300aのFDDに手順1で保存したフロッピーディスクを挿入する。

   ② Management Consoleの「ディスク」を選択してディスク一覧を表示させる。

   ③ ディスク一覧からデバイス名「/dev/fd0」の左にある[詳細]を押す。

   ④ ディスク詳細画面にある[接続]を押す。

3. VC300aに「telnet」でログインする。

   ① Management Consoleの「サービス」で「リモートログイン(telnet)」を起動させる。

   ② 以下のユーザ名/パスワードでログインする。

      ユーザ名:　　admin
      パスワード:　初期導入設定ツールで設定を行ったパスワード

   ③ システム管理者権限を得る。

      $ su
      パスワード:　初期導入設定ツールで設定を行ったパスワード

4. フロッピーディスクにあるファイルを適当な場所にコピーする。(以下 /tmp 配下にコピーするものとして説明します。)

      # cp /mnt/floppy/ダウンロードしたファイル名 /tmp

5. ダウンロードしたファイルを展開する。

      # cd /tmp
      # tar xZf ダウンロードしたファイル名→ libvsapi.so が作成されます

6. 起動中のウイルス監視デーモンをすべて停止させる。

   InterScanコンソールの左側メニューから「Turn On/Off」を選択して起動中(ON)のものをすべて停止(OFF)させてください。

7. 検索エンジンファイルを入れ替える。

      # cd /etc/iscan
      # cp -p /tmp/libvsapi.so .　(展開した検索エンジンをコピーします)
      cp: overwrite `./libvsapi.so'?　y　(yキーを押して上書きコピーを行います)

8. 検索エンジンのバージョンを確認する。

```
# ./vscan -v
Virus Scanner v3.1, VSAPI vx.ｘｘｘ-ｘｘｘｘ
(現在の検索エンジンバージョンが表示されます)
```

9. 手順6で停止させたウイルス監視デーモンを起動させる。

   フロッピーディスクは手順2で[切断]を押してから取り出します。必要に応じて手順3で起動した「リモートログイン(telnet)」を停止させてください。

InterScan VirusWallのユーザー登録

ユーザー登録は非常に大切な作業であり、InterScan VirusWallのユーザー登録を行うと、次のサービスを受けることができます。

- 1年間の無料ウイルスパターンファイルのアップデート
- 1年間の無料サポートサービス
- 製品の更新情報や新製品案内のご提供

ソフトウェアは次の方法で登録できます。

- インターネット経由の登録
- FAXによる登録

インターネット経由のユーザー登録は、非常に高速また便利な方法です。必要な情報を入力して[Register]をクリックしてデータをトレンドマイクロ社に送信するだけで、ウイルスパターンファイルのアップデートのサービスを受けられるようになります。
サポートサービスや情報提供はサポート申し込み書による登録が必要です。

InterScanとインターネットの間にHTTPプロキシサーバが設定されている場合には、InterScan VirusWallでHTTPプロキシサーバを設定する必要があります。詳細については、「HTTPプロキシサーバの使用」を参照してください。

インターネット経由でユーザー登録するには、次の手順に従ってください。

1. Webブラウザを起動して、InterScanコンソールを開き、ブラウザの左側のフレームで、[Pattern Update]をクリックする。

2. [Update Virus Pattern From Internet]ページで、[Register for Virus Pattern Update]をクリックする。

   [Register For Virus Pattern Updates]画面が表示されます。

3. 必要事項をすべて記入する。

   基本ライセンスに添付されているシリアル番号を入力してください。

4. [Register]をクリックして、入力した情報をトレンドマイクロ社に送信する。

   重要

   プログラムからウイルスパターンファイルのアップデートを受信するには、インターネット経由でユーザー登録を実行する必要があります。

E-Mail VirusWallの設定

E-Mail VirusWallは、お使いのネットワーク環境に応じて、さまざまな設定でご利用いただくことができます。
詳細については、基本ライセンスに添付の「InterScan VirusWall管理者ガイド」を参照してください。

[E-Mail Scan Configuraiont]ページの[Main service port]の設定は、E-Mail VirusWallを導入する際のトポロジに依存します。
トポロジの詳細については、管理者ガイドの第2章を参照してください。

ローカルホスト上のsendmailを使用する場合

1. InterScan設定ページを表示し、[Configuration]→[E-Mail Scan]を選択する。
2. [Original SMTP server location]で[Local server]を選択する。
3. オリジナルの sendmailを指定する。

<コマンドモードの場合>

[Command mode]を選択し、ローカルホスト上の sendmail プログラムのパスを指定します。必要であればパラメータも指定します(例: /usr/lib/sendmail -bs)。

<デーモンモードの場合>

[Daemon mode]を選択し、[Port Number]にオリジナルの sendmailで使用するポート番号を指定します。

デーモンモードを利用するためには本装置上でsendmailを起動する必要がありますが、Management Consoleからsendmailの起動を行うことはできません。ローカルホスト上のsendmailを使用する場合にはコマンドモードを使用してください。起動設定や設定ファイル(sendmail.cf)の内容変更によるsendmailの動作についてはサポート対象外となります。

リモートサーバ上のSMTPサーバを使用する場合

1. InterScan 設定ページを表示し、[Configuration]→[E-Mail Scan]を選択する。
2. [Original SMTP server location]で[Remote server]を選択する。
3. オリジナルのSMTPサーバを指定する。

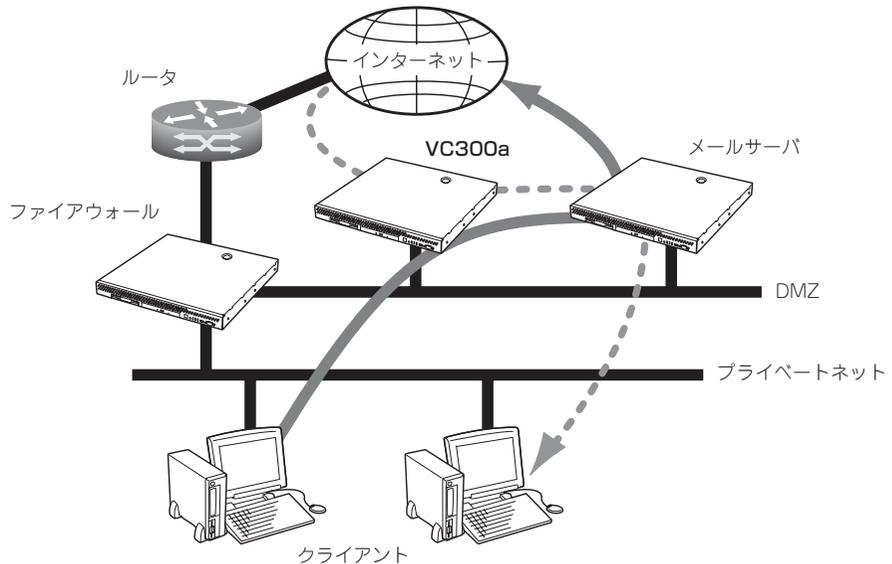
[Hostname]にオリジナルのSMTPサーバが動作するリモートサーバのサーバ名またはIPアドレスを指定します(例: remoce.com)。
[Port number]にオリジナルのSMTPサーバが使用するポート番号を指定します。ポート番号には、ほとんどの場合、25を指定します。
次に例を示します。

mailserver 25
mailserver.yourcompany.com 25
123.12.12.123 25

InterScan VirusWallの動作

E-Mail VirusWallは、ポート番号25でSMTPトラフィックを受信後、対象となるトラフィックのウイルスを検索し、指定されたポート(ここでは25)を使用して、[Original SMTP server location]で指定された SMTPサーバにルーティングします。

E-mail VirusWallの導入例

● **メールサーバが非武装地帯(DMZ)上にある場合**

設定方法1

1. メールサーバのIPアドレス/ホスト名とVC300aのIPアドレス/ホスト名を入れ替える。

2. クライアントメーラーが設定する受信メール(POP)サーバを入れ替え後のメールサーバのIPアドレス/ホスト名に変更する。

3. VC300aがメールをメールサーバに配送するように設定する。

   E-Mail Scan ConfigurationのOriginal SMTP server location: で Remote server: を選択し、Hostname: とPort Number: にメールサーバのホスト名(IPアドレス)とポート番号を指定します。

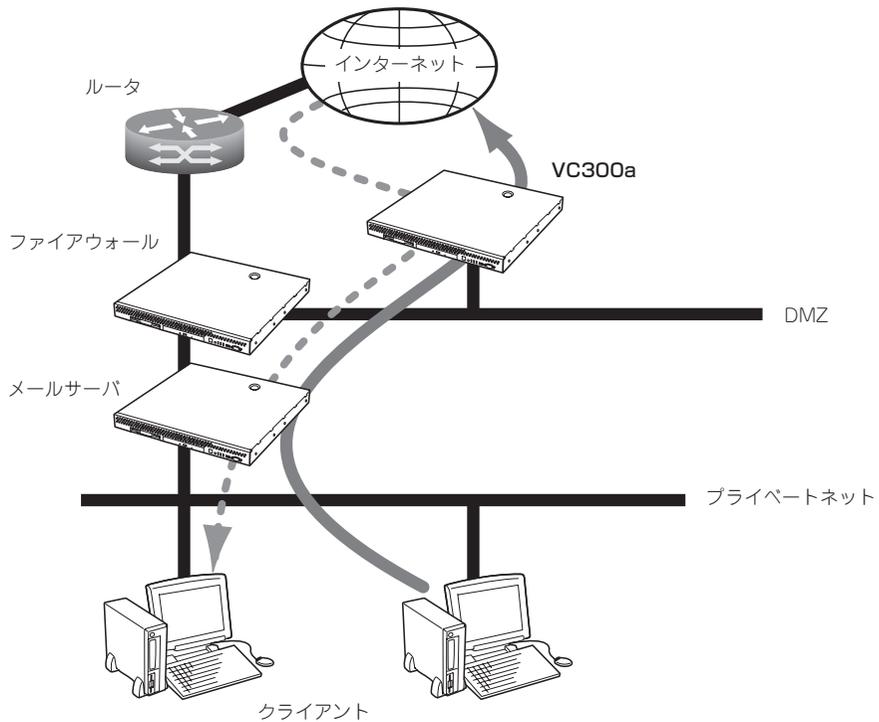
設定方法 2

1. DNSのMXレコードをVC300aへ変更してインターネットからのメールの配送先をVC300aとする。

2. クライアントメーラーが設定する送信メール(SMTP)サーバをVC300aに変更する。

3. VC300aがメールをメールサーバに配送するように設定する。

   E-Mail Scan ConfigurationのOriginal SMTP server location: で Remote server: を選択し、Hostname: とPort Number: にメールサーバのホスト名(IPアドレス)とポート番号を指定します。

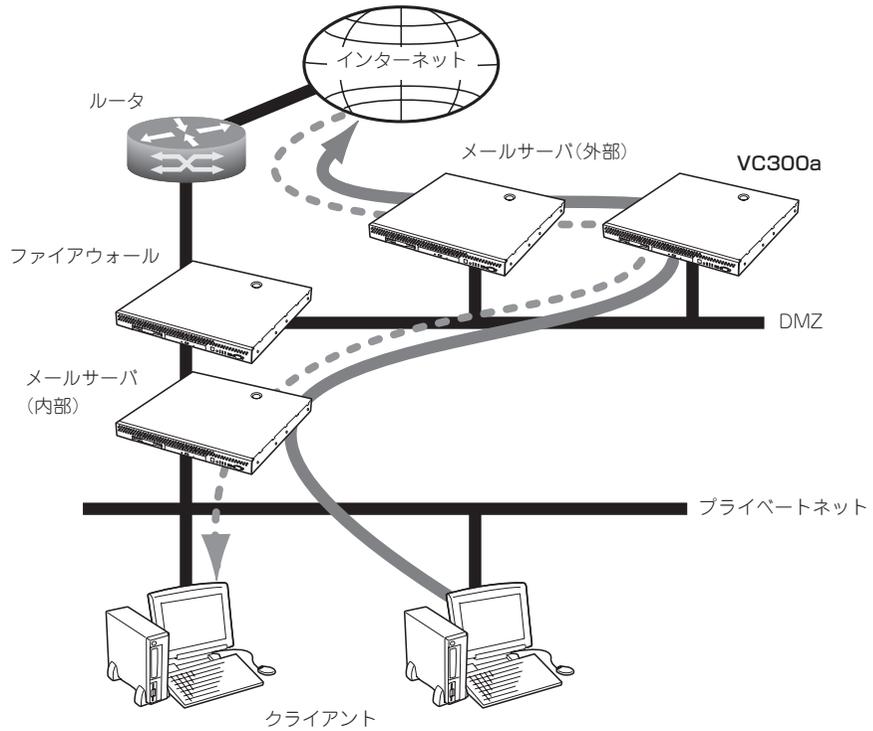
● メールサーバが内部にある場合

設定方法

1. DNSのMXレコードをVC300aへ変更する。

2. メールサーバが外部へのメールをVC300aに配送するように変更する。

3. VC300aが内部へのメールはメールサーバへ、外部へのメールはインターネットへ配送するように設定する。

   E-Mail Scan ConfigurationのOriginal SMTP server location: で Local server: および Commande mode: を選択します。Management Consoleの「配送設定(sendmail)」にある「静的配送の設定」で、内部ドメイン名と転送先のメールサーバを指定します。

● メールサーバが外部と内部にある場合

設定方法

1. 外部メールサーバが内部へのメールをVC300aに配送するように変更する。

2. 内部メールサーバが外部へのメールをVC300aに配送するように変更する。

3. VC300aが外部メールサーバからのメールは内部メールサーバへ、内部メールサーバからのメールは外部メールサーバへ配送先するように設定する。

   E-Mail Scan ConfigurationのAdditional Email OptionsにあるMultiple relay direction: を有効とし、 以下の設定を行います。senderをチェックし、senderに内部メールサーバのホスト名あるいはIPアドレスを、recipientに外部メールサーバのホスト名あるいはIPアドレスを指定します。次のsenderをチェックし、senderに外部メールサーバのホスト名あるいはIPアドレスを、recipientに内部メールサーバのホスト名あるいはIPアドレスを指定します。

Web VirusWallの設定

Web VirusWall は、お使いのシステムの設定に従って独自のプロキシサーバとして設定することも、既存の HTTPプロキシサーバと併用することもできます。システムの設定に応じて、 InterScanコンソールの[HTTP Scan Configuration]ページで、[InterScan acts as a proxy itself]または[Other (server and port)]のどちらかを選択し、[InterScan HTTP Proxy port (connects to browser)]にポート番号(通常は80)を指定します。

重要

Web VirusWallでFTPトラフィックを検索する場合は、クライアント側のWebブラウザで、Web VirusWallをFTPプロキシとして使用するように設定する必要があります。

オリジナルHTTPサーバの指定: [Original HTTP server location]

1. 管理コンソールで[Configuration]→[HTTP Scan]を選択し、[InterScan HTTP Proxy port...]に、Web VirusWallがクライアントからの接続を監視するポート番号を入力する。

   通常は80を指定します。

2. [Original HTTP server location]で、[InterScan acts as a proxy itself]、または[Other (server and port)]を選択して、サーバ名(または IPアドレス)とポート番号を指定する。

   [InterScan acts as a proxy itself]

   ネットワーク上に既存の HTTPプロキシサーバがなく、Web VirusWallをシステム全体のHTTPプロキシサーバとして使用する場合、または Web VirusWallを論理上インターネットとプロキシサーバの間に配置する場合には、このオプションを選択します。

   [Other (server and port)]

   ネットワーク上に既存のHTTPサーバがある場合には、このオプションを選択し、サーバ名とポート番号を入力します。Web VirusWallでは、ここで指定されたマシンに対するすべてのHTTPトラフィック、およびそのマシンからのすべてのHTTPトラフィックについて、ウイルス検索を行います。

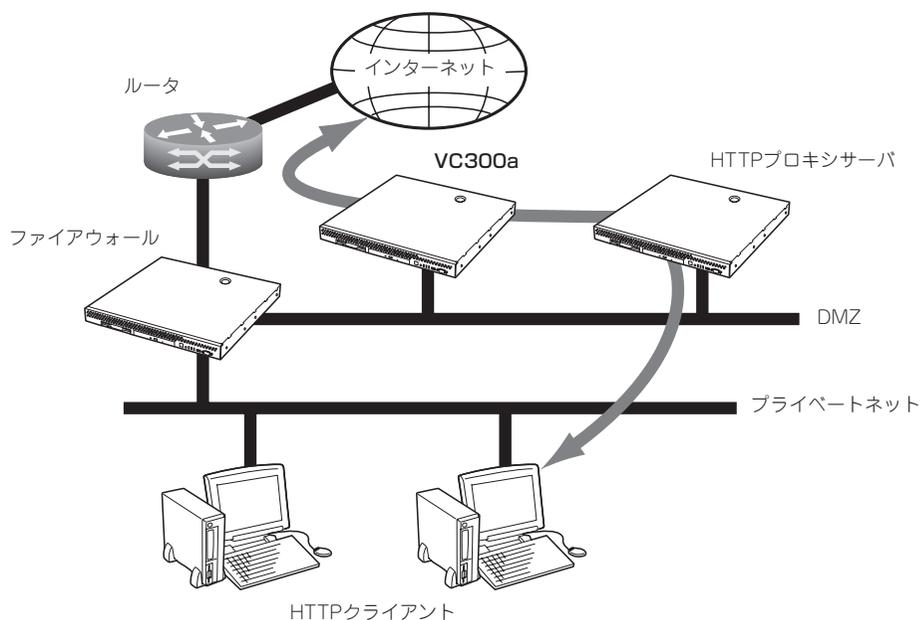
3. [Other (server and port)]に、 HTTP デーモン(in.httpd)を実行するマシンのドメイン名またはIPアドレスを入力します。次に例を示します。

   proxy.yourcompany.com 80
   123.12.13.123 80

テスト

Telnetまたは同様のプログラムを使用して、上記の設定で指定したInterScanのIPアドレスおよびポート番号に対して、Telnetを実行します。サーバからの応答の内容を確認することで、ほとんどの設定を識別し、解決することができます。

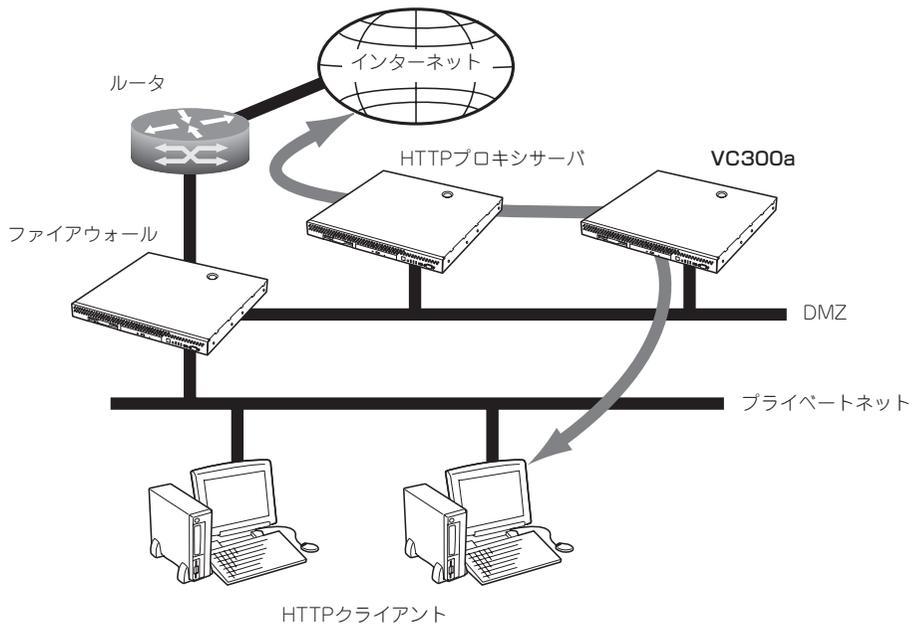
Web VirusWallの導入例

● HTTPプロキシサーバの上位にVC300aを設置する場合

設定方法

1. HTTPプロキシサーバの上位プロキシサーバとしてVC300aを設定する。

2. VC300aが直接インターネットを参照するプロキシサーバとして動作するよう設定する。

   HTTP Scan ConfigurationのOriginal HTTP server location: でInterScan acts as proxy itself. を選択します。

● HTTPプロキシサーバの下位にVC300aを設置する場合

設定方法

1. クライアントで利用するブラウザのHTTPプロキシサーバとしてVC300aを設定する。

2. VC300aの上位プロキシサーバとしてHTTPプロキシサーバを設定する。

   HTTP Scan ConfigurationのOriginal HTTP server location: でOther (server and port): を選択し、HTTPプロキシサーバのホスト名とポート番号を入力します。

FTP VirusWallの設定

[FTP Scan Configuration]ページで指定する FTPサーバの場所とポート番号は、FTP VirusWallが独自のプロキシサーバとして導入されるかどうか、既存のFTPサーバと併用するように導入されるかどうか、などに依存します。

オリジナルFTPサーバの指定: [Original FTP server location]

1. 管理コンソールで[Configuration] →[FTP Scan]を選択する。

2. [Main service port]にFTP VirusWallでクライアントからの新しい接続を監視するポートの番号を指定する。

   通常は21を指定します。

3. [Use user@host]または[Server location]のいずれかを選択する。

   [Server location]を選択した場合は、FTPサーバのパスとポート番号を設定してください。

[Use user@host]: ネットワークで唯一の FTPサーバとして動作する場合

FTP VirusWallをシステムのFTPサーバとして使用する場合は、[Use user@host]を選択してください。クライアントからは常にInterScanにFTP接続し、InterScanでは要求されたサイトに対する接続を確立します。クライアントでユーザ名とパスワードの入力が要求された際に、ユーザ名に対象となるドメインのドメイン名をつけることを忘れないでください。たとえば、ユーザjohnがwidgets.comにFTP接続する場合の例を示します。

- widgets.comに直接接続する場合

  ユーザ名:　john
  パスワード:　opensesame

- FTP VirusWallを介して接続する場合

  ユーザ名:　john@widgets.com
  パスワード:　opensesame

[Server location]: ネットワーク上に既存の FTP サーバがある場合

ネットワーク上に既存のFTPサーバがある場合には、[Server location]を選択し、テキストボックスにサーバのパスとポートを入力します。FTP VirusWallでは、ここで指定されたマシンに対するすべてのFTPトラフィック、およびそのマシンからのすべてのFTPトラフィックについて、ウイルス検索を実行します。

4. [Original FTP server location]の[Server location]に、既存のFTPサーバのホスト名(またはIPアドレス)とポート番号を入力する。

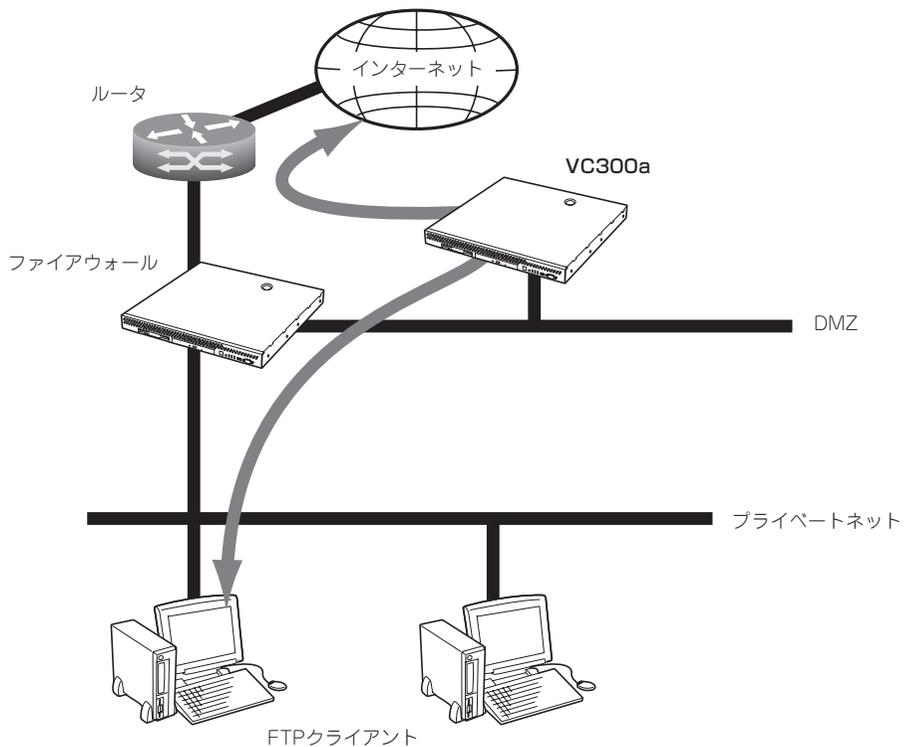
   次に例を示します。

   ftp-server.yourcompany.com 21
   123.12.13.123 21

テスト

Telnetまたは同様のプログラムを使用して、前述の設定で指定した InterScanのIPアドレスおよびポート番号に対して、Telnetを実行します。サーバからの応答の内容を確認することで、ほとんどの設定を識別し、解決することができます。

FTP VirusWall の導入例

● ネットワーク内にFTPプロキシサーバが存在しない場合

設定方法

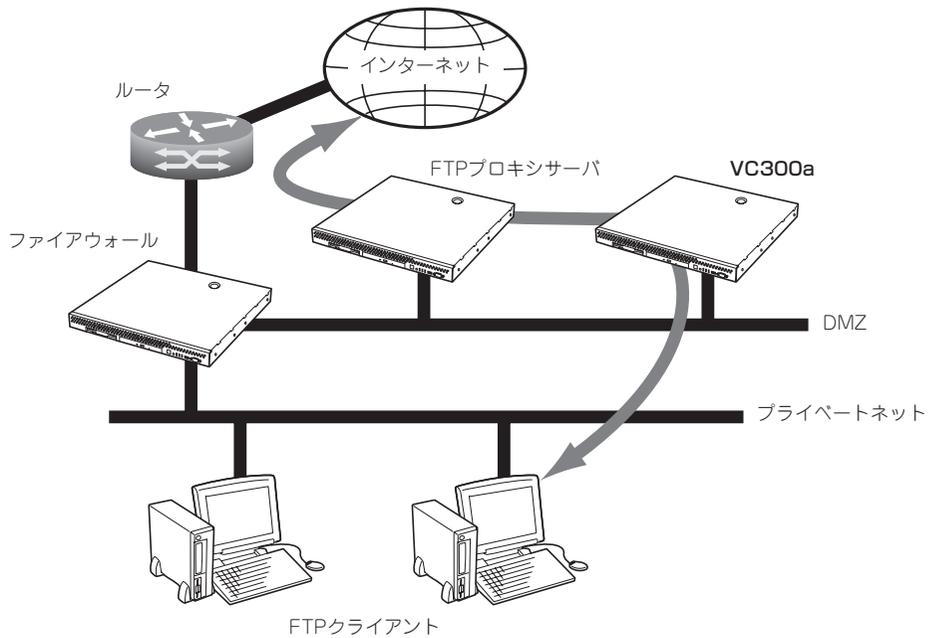
1. VC300aが直接インターネットを参照するFTPサーバとして動作するよう設定する。

   FTP Scan Configuration の Original FTP server location: でUse user@host: を選択する。

2. クライアントからFTPを利用する場合、VC300aに接続を行い、ユーザ名には ユーザ名@FTPサーバのホスト名 の形式で入力する。

   ー　ftpserver.com にユーザ名(user)、パスワード(pass)で接続する場合

   ユーザ名:　user@ftpserver.com
   パスワード:　pass

● **FTPプロキシサーバが存在する場合**

設定方法

1. VC300aの上位プロキシサーバとしてFTPプロキシサーバを設定する。

   FTP Scan ConfigurationのOriginal FTP server location: で Server location: を選択し、FTPプロキシサーバのホスト名とポート番号を指定する。

2. クライアントで利用するFTPクライアントのFTPプロキシサーバとしてVC300aを設定する。

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro/doc/users.pdf

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

システム情報のバックアップ

システムのセットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

「保守・管理ツールCD-ROM」からシステムを起動して操作します。「保守・管理ツールCD-ROM」から起動させるためには、事前にセットアップが必要です。5章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. 本体に添付の「保守・管理ツールCD-ROM」から「オフライン保守ユーティリティ」を起動する。

   「保守・管理ツールCD-ROM」の使い方については5章を参照してください。
3. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理PCに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。

管理PCのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「Management Workstation Application（MWA）」が用意されています。
これらのアプリケーションを管理PCにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerとMWAのインストールについては5章、または「保守・管理ツールCD-ROM」内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムクラッシュなどの原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

保守用パーティションの作成

「保守用パーティション」とは、装置の維持・管理を行うためのユーティリティを格納するためのパーティションで、55MB程度の領域を内蔵ハードディスク上へ確保します。
システムの信頼性を向上するためにも保守用パーティションを作成することをお勧めします。保守用パーティションは、添付の「保守・管理ツールCD-ROM」を使って作成します。詳しくは5章を参照してください。
保守用パーティションを作成するプロセスで保守用パーティションへ自動的にインストールされるユーティリティは、「システム診断ユーティリティ」と「オフライン保守ユーティリティ」です。

システムの再インストール

再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールには、本体添付の「バックアップCD-ROM」と「バックアップCD-ROM用インストールディスク」が必要です。
「バックアップCD-ROM用インストールディスク」を3.5インチフロッピーディスクドライブに、「バックアップCD-ROM」をCD-ROMドライブにそれぞれ挿入し、POWERスイッチを押して電源をONにします。

このとき、前面のシリアルポートB(COM B)に管理PCを19,200bpsの転送速度で接続すると、管理PCからログを参照することができます。

しばらくすると「バックアップCD-ROM用インストールディスク」から設定情報を読み取り、自動的にインストールを実行します。

重要

このとき、確認等は一切行われずにインストール作業が開始されるため、十分注意してください。

約30分程度でインストールが完了します。インストールが完了したら、CD-ROMが自動的にイジェクトされます。CD-ROMとフロッピーディスクの両方をドライブから取り出してください。

40分以上待っても、CD-ROMがイジェクトされず、CD-ROMへのアクセスも行われていない場合は再インストールに失敗している可能性があります。リセットして、CD-ROM/フロッピーディスクをセットし直して再度インストールを試みてください。それでもインストールできない場合は、保守サービス会社、またはお買い上げの販売店までご連絡ください。

初期導入設定用ディスクの作成

前述の「初期導入設定用ディスクの作成」を参照してください。すでに初期導入設定用ディスクを作成している場合は、パスワード情報の設定のみ再度設定し直してください。ただし、設定内容を変えたいときは、新たに初期導入用設定ディスクを作り直してください。

システムのセットアップと確認

前述の「システムのセットアップ」、「セットアップの確認」を参照してください。

ESMPRO/ServerAgentのセットアップ

「システムの再インストール」でESMPRO/ServerAgentは自動的にインストールされますが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro/doc/users.pdf

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)も自動的にインストールされます。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

セキュリティパッチの適用

最新のセキュリティパッチは、以下のURLよりダウンロード可能です。

http://www.express.nec.co.jp/care/index.asp

定期的に参照し、適用することをお勧めします。